Oct. 2010 CHINESE JOURNAL OF ENGINEERING MATHEMATICS Vol. 27 No. 5

Article ID:1005-3085(2010)05-0939-04

A New Lightweight Authentication Protocol for the RFID System*

NIU Zhi-hua[1,2], WU Xue-hui[1]

(1- School of Computer Engineering and Science, Shanghai University, Shanghai 200072;
2- State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100080)

Abstract: Radio frequency identification (RFID) is poised to supplant the barcodes in the near future. Its information storage capacity as well as its ability to transfer information are superior barcodes. However, the user's privacy invasion and system security threats are increasingly concerned by users. The implementation of security protocols in RFID is challenging as they are highly resource constrained and unable to perform strong from cryptography. Recently several authentication protocols have been proposed to prevent unauthorized tracking, impersonation and cloning etc. In this paper, a new efficient mutual authentication protocol is proposed to offer an adequate security level for certain applications, as tag in this protocol only has hash function and exclusive-or operation while reader or server takes on the most calculations including the generation of the random number and the computing of the encryption/decryption. Compared with other protocols, the protocol presented here achieves in resisting privacy leakage, spoofing and replaying attack etc, and is feasible to the low-cost, limited computation RFID system.

Keywords: cryptology; lightweight; RFID; mutual-authentication

Classification: AMS(2000) 11T71 **CLC number:** TN918.4 **Document code:** A

1 Introduction

RFID[1] is currently considered as a substitution for an optical bar code system in the near future. There are three key elements within a RFID system: RFID tag, or transponder, to carry object-identifying data; RFID reader, or transceiver[2], to read and write tag data; Back-end server, or database, to associate records with tag data collected by readers.

However, before pervasive deployment with RFIDs, several security risks and potential privacy problems should be resolved. Because the communication channel is insecure and the implementation of well-known cryptographic algorithms remains difficult due to the restricted computational power. Simply eavesdropping the messages transmitted between the reader and the tag, the attacker can obtain the unique information of the tag, and also can track tag without any authorization.

Received: 27 Oct 2008. **Biography**: Niu Zhihua (Born in 1976), Female, Ph.D. Research field:
Accepted: 19 Feb 2009. information security and cryptography.

***Foundation item:** The National Natural Science Foundation of China (60903187; 60970006); the Shanghai Leading Academic Discipline Project (J50103); the Shanghai Municipal Education Commission Development Foundation under Grant (A10-0108-06-002); the Shanghai Municipal Education Commission Innovation Project (10YZ13).

2 Background and related work

Weis *et al*[3] proposed Hash-lock protocol and the randomized hash-lock protocol. Although the Hash-lock scheme offers good reliability at low cost, an adversary can easily track the tag via its metaID. While the randomized hash-lock scheme can deter tracking, it allows the location history of the tag to be traced if the secret information is revealed.

Ohkubo *et al*[4] used a low cost hash-chain mechanism to defeat the tracing problem. Although this scheme uses two different one-way hash functions, an attacker can still query the tag then replay the tag's response to authenticate itself to a valid reader.

Vajda *et al*[5] proposed a set of lightweight security protocols. However, these protocols rely on the existence of a shared secret which makes it problematic for the reader to determine what secret corresponds to what tag. Moreover, they do not address the problem of reader-to-tag authentication and no attempt is made to prevent from tracking of the tags.

Henrici *et al*[6] proposed the hash-based ID variation protocol in which the ID of the tag varies in each session. However, the attacker could still track the tag with the fixed hashed ID.

3 Our proposed protocol

Before describing our protocol in detail, we give the definition of the notations as summarized in Table 1 and assume that all of the one-way hash functions are the same in Figure 1.

Table 1: Notations

Notation	Interpretation
h( )	One-way hash function
E_k( )	Symmetric-key encryption function with the key k
D_k( )	Symmetric-key decryption function with the key k
RNG	Random number generation
K	Shared random secret between T and B
r	Pseudo-random number generated by RNG
D	A database of back-end server
ID	The static tag-identification number
DATA	All application related data of T

Step 1 R generates a fresh random nonce, r, with the RNG, and randomizes it with the one-way hash function, $S = h(r)$. R sends S to the queried T. S is used to authenticate the validity of R. With S, the man-in-the-middle attack is prevented against an active attacker.

Step 2 When queried, T sends M and N to R. M is to verify the legitimate R, and prevent the forgery from the passive eavesdropping.

Step 3 R simply forwards M, N, S and r to B. At first, B verifies whether the forwarded r is valid or not by comparing S with $h(r)$. The man-in-the-middle attack by the illegitimate R and a passive eavesdropper can be prevented. If R is valid, for each tuple (ID, K) in D, B verifies that $M \bigoplus K$ equals $h(ID \| h(r))$ and N equals $h(M \bigoplus h(r))$. If no tuple is found, the

tag is rejected. Similarly, the replay attack can be also detected and prevented. If B successfully finishes the authentication process, B generates C.

Step 4 B encrypts the corresponding DATA using the key k, then replies C and E_k (DATA). Thus, DATA of T is securely obtained only by the legitimate R. Then, B makes its shared key, K, randomized simply by Xoring with C.

Step 5 R forwards C to T. T verifies the forwarded C, calculates $h(K)$ and compares it with C. If matched, the mutual authentication is finally succeeded, and T, updates the shared secret K. Otherwise, T will not updates it in a case the replay attack to T occurs.

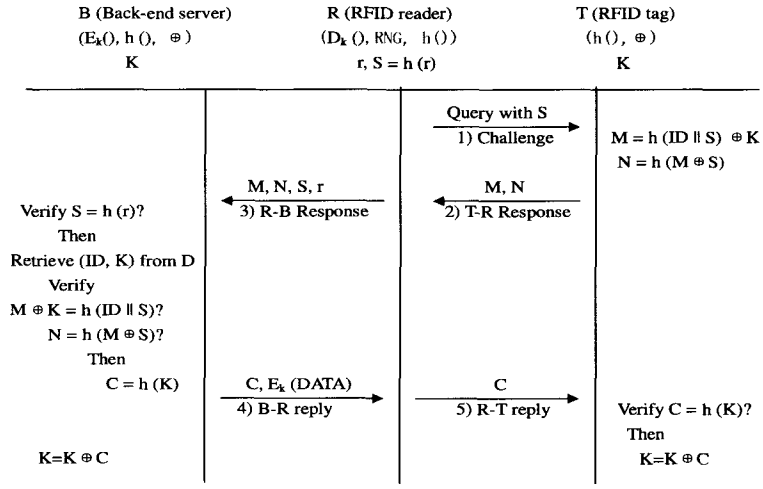

Figure 1: Our Proposed Protocol

4 Security analysis

The user's privacy mainly means the location information or the tag information of the owner. In our scheme the tag does not store user's privacy information, and the tag ID is hidden in the message M, so that data confidentiality is guaranteed. Tag never directly emits the ID in a plaintext form. In each session, the tag sends out a different bit string because of nonce r. It is infeasible for malicious parties to use a compatible reader to track the tag holder. Therefore, tag anonymity is guaranteed. Based on the mutual authentication, our protocol guarantees the data integrity between T and B.

As mentioned above, a forgery or replay attack is not possible because our proposal is based on a mutual authentication and the random nonce r as well as key K is updated for each session. Attackers have no idea of which operations have been used and therefore the simple copy of information of the tag by eavesdropping is also not possible. Table 2 shows the comparison with some existing protocols.

Table 2: Comparison (Y means satisfied, N means not)

	Privacy	Anonymity	Data Integrity	Mutual Authentication	Resist to Replay Attack	Forgery Resistence
Weis *et al*	N	N	Y	N	N	N
Ohkubo *et al*	Y	Y	N	N	N	Y
Vajda *et al*	N	Y	Y	N	N	N
Henrici *et al*	Y	N	Y	N	N	N
our scheme	Y	Y	Y	Y	Y	Y

5 Conclusions

In this paper, we have proposed a lightweight authentication protocol for low-cost RFID tags. Our scheme achieves the data security criterion, the privacy requirements of tag anonymity and intractability, and the low-cost implementation requirement. From the analysis of the proposed protocol, we conclude that it is completely feasible in a low-cost RFID environment.

References:

[1] RFID Journal. Gillette to purchase 500 million EPC tags[OL]. http://www.rfidjournal.com, January 2003
[2] Sarma S, Weis S, Engels D. RFID Systems and Security and Privacy Implication: Auto-ID Center[M]. Berlin Heidelberg: Springer-Verlag, 2003
[3] Weis S, Sarma S, Rivest R, *et al*. Security and privacy aspects of low-cost radio frequency identification systems[C]// 1st Intern. Conference on Security in Pervasive Computing (SPC), 2003
[4] Ohkubo M, Suzuki K, Kinoshita S. Cryptographic approach to privacy-friendly tags[C]// RFID Privacy Workshop, MIT, 2003
[5] Istvan Vajda A, levente Buttyan. Lightweight authentication protocols for low-cost RFID tags[C]// 2nd Workshop on Security in Ubiquitous Computing, 2003
[6] Dirk Henrici, Paul Muller. Hash-based enhancement of location privacy for radio frequency identification devices using varing identifiers[C]// Workshop on Pervasive Computing and Communications Security, 2004

一种新的轻量级的RFID认证协议

牛志华[1,2], 吴学慧[1]

(1- 上海大学计算机工程与科学学院，上海 200072;
2- 中国科学院研究生院信息安全国家重点实验室，北京 100080)

摘 要: 无线射频识别技术(RFID)有望在不久的将来取代条形码系统，它的信息存储量以及传输信息的能力相比条形码都有明显的优势。然而，由此引发的用户隐私入侵和系统安全威胁一直是用户日益关注的问题。由于其设备的资源受限，以及无法执行强加密算法，因此于RFID系统中安全协议的执行是一个极大的挑战。为此，近来许多认证协议已被提出以防止未经授权的定位跟踪、检测、假冒、克隆等。本文提出了一种新的有效的轻量级射频识别认证协议，对于某些应用，它已能提供足够的安全级别。该协议中标签只需执行hash和异或运算而阅读器和后台服务器承担大部分的运算量包括伪随机数的产生以及加解密的运算。相比于其他协议，我们实现了防止隐私泄露、伪装等安全攻击的特点，适合于低成本、低计算量的RFID系统。

关键词: 密码学；轻量级；无线射频识别；双向认证